

*Federal Network Security  
Federal Interagency Technical Reference Architectures*

# Electronic Mail Gateway Security Reference Architecture

*Version 1.0*

*12/12/2011*



Department of Homeland Security  
National Cyber Security Division  
Federal Network Security  
Network & Infrastructure Security

## Revision History

Date	Version	Description	Approved By
12/12/2011	1.0	Initial Version	CS&C

## Table of Contents

<b>ACKNOWLEDGEMENTS.....</b>	<b>1</b>
STAKEHOLDERS .....	1
PARTICIPANTS.....	1
<b>1    PURPOSE AND SCOPE.....</b>	<b>2</b>
<b>2    ELECTRONIC MAIL GATEWAY ARCHITECTURAL COMPONENTS .....</b>	<b>2</b>
2.1    SYSTEM OVERVIEW .....	3
2.2    INBOUND MAIL TRANSFER AGENT (MTA).....	4
2.3    OUTBOUND MAIL TRANSFER AGENT (MTA).....	4
2.4    BILATERAL MAIL RELAY/EXCHANGER (MTA).....	5
2.5    MOBILE MESSAGING .....	5
<b>3    SECURITY PATTERNS .....</b>	<b>5</b>
3.1    SECURITY USE CASES .....	5
3.1.1 <i>Pattern 1: Inbound Electronic Mail</i> .....	5
3.1.2 <i>Pattern 2: Outbound Electronic Mail</i> .....	6
3.1.3 <i>Pattern 3: Mobile Messaging</i> .....	6
3.2    SECURITY ARCHITECTURE COMPONENTS .....	6
3.2.1 <i>Pipeline Structure</i> .....	7
3.2.2 <i>Data Loss Prevention</i> .....	11
3.2.3 <i>Content Compliance</i> .....	11
3.2.4 <i>Malware Filtering</i> .....	11
3.2.5 <i>Domain Validation</i> .....	12
3.2.6 <i>SPAM Filtering</i> .....	12
3.2.7 <i>Agency Specific Modules</i> .....	12
3.3    SECURITY REQUIREMENTS.....	13
3.3.1 <i>Inbound Gateway Mail Transfer Agent (MTA) Requirements</i> .....	13
3.3.2 <i>Outbound Gateway Mail Transfer Agent (MTA) Requirements</i> .....	13
3.3.3 <i>Mail Submission Agent Requirements</i> .....	14
3.3.4 <i>Mail Delivery Agent Requirements</i> .....	14
3.3.5 <i>Mail User Agent Requirements</i> .....	14
3.3.6 <i>Domain Name System (DNS) Requirements</i> .....	14
3.3.7 <i>Firewall Requirements</i> .....	15
3.3.8 <i>Logging Requirements</i> .....	15
3.3.9 <i>System Monitoring and Control</i> .....	16
3.3.10 <i>Archiving Requirements</i> .....	16
3.3.11 <i>Audit Requirements</i> .....	16
<b>4    SYSTEMIC THREATS &amp; MITIGATIONS .....</b>	<b>16</b>
<b>5    SECURITY CONFIGURATION.....</b>	<b>22</b>
<b>6    APPENDIX A: SAMPLE SPF RECORDS .....</b>	<b>23</b>
<b>7    APPENDIX B: SAMPLE DKIM DOMAIN RECORD ENTRY .....</b>	<b>24</b>
<b>8    APPENDIX C: ACRONYMS – COMMON ABBREVIATIONS.....</b>	<b>26</b>
<b>9    APPENDIX D: GLOSSARY – COMMON TERMS AND DEFINITIONS.....</b>	<b>28</b>
<b>10   APPENDIX E: SELECTED EXISTING GUIDANCE.....</b>	<b>32</b>
10.1    LEGISLATION .....	32
10.2    POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA.....	32

10.3	STANDARDS.....	32
10.4	GUIDELINES .....	33
10.5	IETF RFCs .....	36

Figures

FIGURE 1 - MAIL SYSTEM FUNCTIONAL COMPONENTS..... 4

FIGURE 2 - SMTP TRANSFER MODEL ..... 7

FIGURE 3 - INBOUND MTA PIPELINE..... 8

FIGURE 4 - OUTBOUND MTA PIPELINE..... 10

## Acknowledgements

This document is the product of a multi-agency collaboration to provide guidance for the successful and secure implementation of Electronic Mail Gateways at Federal civilian agencies. It further expands on the Critical and Recommended Content Filtering capabilities found in the Trusted Internet Connections (TIC) Reference Architecture v2.

This document will be reviewed annually and updated when necessary to incorporate required capabilities and applicable interoperability standards.

## Stakeholders

All Federal civilian agencies

Office of Management and Budget (OMB), Office of E-Government and Information Technology

Federal Chief Information Office (CIO) Council

Federal Small Agency CIO Council

Department of Homeland Security (DHS) National Cyber Security Division (NCSD)

Federal Systems Security Governance Board (FSSGB)

DHS Information Systems Security Line of Business (ISS LoB)

DHS United States Computer Emergency Readiness Team (US-CERT)

General Services Administration (GSA) Information Technology Infrastructure Line of Business (ITI LoB)

## Participants

Name	Agency	Name	Agency
Jim Quinn	DHS	Eric Pratsch	SRA-Touchstone
Marilyn Rose	DHS	Robert Moore	SRA-Touchstone
Oscar Ahumada	DHS	Marcos Evangelista	STATE
Sean Donelan	DHS	Janice Ousley	Treasury/IRS
Arthi Appulingam	EDU	Stewart Grossman	Treasury/IRS
David Elliot	EDU	Homa Zarrinnahad	Treasury/OCC
Pete Batista	FCC	Tim Arnold	USDA
Daniel Sheehan	Indian Health Service		
Jeff Schwefler	MITRE		
Carl Beaudry	SRA International		

## 1 Purpose and Scope

On April 15, 2011, the White House released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which envisions the establishment of secure online identity functionality as part of an overall cyber security strategy. The purpose of the Mail Gateway Reference Architecture is to improve and standardize the Electronic Mail Gateways currently in use by the Federal Civilian Government, help Departments/Agencies (D/As) comply with FISMA mail security requirements and to improve the Federal Government's overall security posture by reducing electronic mail vulnerabilities.

This document is a reference that provides insight and guidance for D/As implementing an electronic mail gateway. This document is descriptive in nature, recognizing that many organizations face unique challenges that do not lend themselves to a "one size fits all" solution. Unlike a Target Architecture, a Reference Architecture does not mandate specific solutions, but rather identifies a range of workable modular solutions. The intent is to enable agencies to leverage existing best practice solutions when implementing electronic mail gateways. The reference architecture will align with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the evolving Anti-Phishing policy, and the National Cyber Security Strategy while factoring in the context of each organizations respective missions, programs, and initiatives.

This document is intended for use by Federal civilian agencies. The information in this document is based upon collaboration with multiple agencies, the definitions and requirements in the Federal Information Systems Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance and standards, Trusted Internet Connection (TIC) Reference Architecture v2, Office of Management and Budget (OMB) memoranda, and evolving national cyber security policies.

## 2 Electronic Mail Gateway Architectural Components

An Electronic Mail Gateway provides the interface between federal agencies' internal mail systems and the mail systems of other federal agencies or Internet mail systems. The gateway processes inbound and outbound mail messages. The complete mail ecosystem which encompasses the mail gateway as well as other components is represented by:

- Mail User Agents (MUAs)/e-mail clients
- Mailbox hosts
- Mail Submission Agents (MSAs)
- Mail Delivery Agents (MDAs)
- Mail Transfer Agents (MTA) both inbound and outbound
- Mail Exchangers
- Mobile messaging servers

- Applications Servers

The electronic mail gateway reference architecture focuses on the MTAs (Figure 1 filled in black) but for architectural completeness the boundaries to the other components are included here.

## 2.1 System Overview

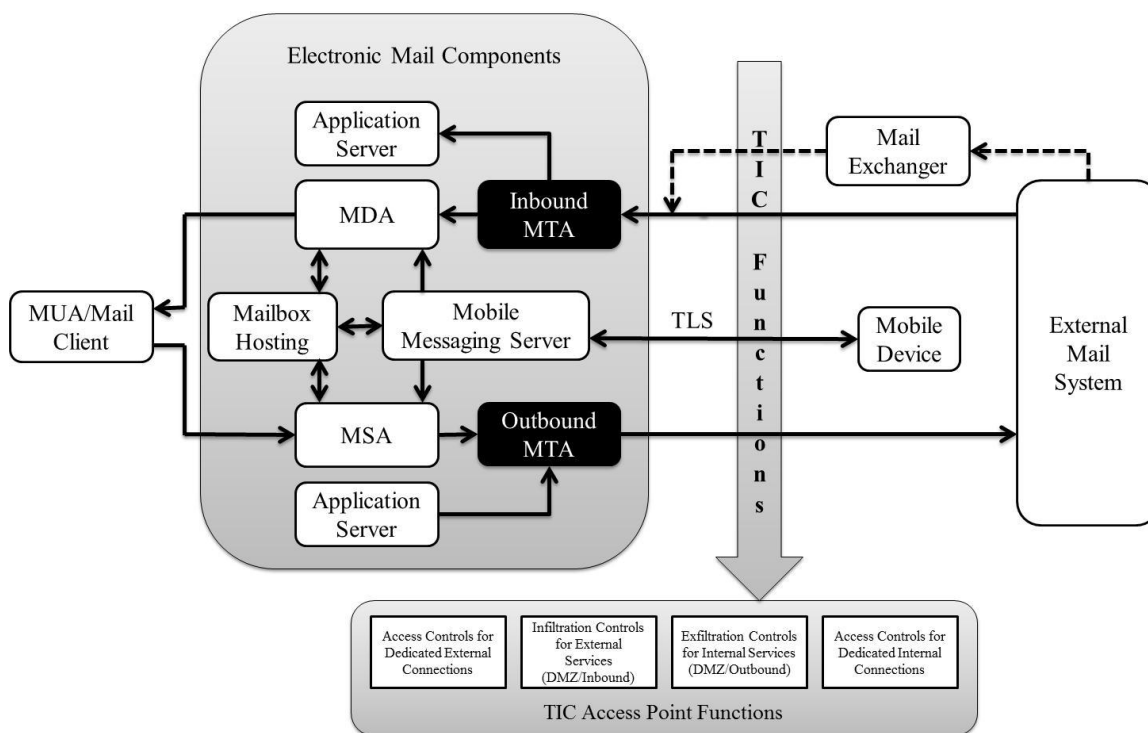
The electronic mail system provides both inbound and outbound mail transactions.

For the outbound transaction, the electronic mail client/MUA provides the user interface, the MSA stores and forwards electronic mail messages to the MTA which, in turn, acts as a proxy between the MSAs and external mail servers.

For the inbound transactions, the MTA receives the messages, the MDA stores the messages, and MUA/mail client provides user access to the message stores. The mobile messaging server provides a secure connection between the mobile messaging device and the MDA and MSA.

Security controls placed on the inbound and outbound MTA pipelines are applied to both mobile and traditional mail transactions. Agency-hosted applications requiring the ability to send email are considered application servers which may deliver outbound mail to either the MSA or the outbound MTA. Application servers may also receive inbound email from either the MDA or inbound MTA. For completeness, mailbox hosting is depicted as a capability connected to the MSA and MDA.

The Electronic Mail Gateway is divided into inbound and outbound MTA pipelines. The relationship of the components and the alignment with the TIC Reference Architecture v2 is depicted in *Figure 1* below. The focus of the Electronic Mail Gateway reference architecture is to describe the functions of inbound and outbound MTAs with reference to the other components of the mail handling system. In addition, the Mail Gateway Reference Architecture relies on functionality described in the Domain Name System (DNS) Security Reference Architecture to discover both internal and external mail handling hosts and the functionality described in the TIC Reference Architecture v2 to provide DMZ functionality.



**Figure 1 - Mail System Functional Components**

## 2.2 Inbound Mail Transfer Agent (MTA)

The inbound MTA processes all mail originating from outside the federal agencies' network. For the Electronic Mail Gateway reference architecture, the enclave represents all users operating within the federal agencies network to include users that are connected by a Virtual Private Network (VPN) or other form of remote connection. The inbound MTA performs functions such as domain validation, spam filtering, malware filtering, and any other agency unique modules. Based on the findings of each function, the MTA will make a disposition decision for each inbound mail transaction. Depending on the sender's security capabilities and receiver's security requirements, the inbound MTA will enable server to server mandatory and/or opportunistic encryption services.

## 2.3 Outbound Mail Transfer Agent (MTA)

The outbound MTA processes all mail originating from inside the federal agencies' enclave. The purpose of the outbound MTA is to provide domain validation, content compliance, data loss prevention, malware filtering, and any other agency unique modules. By providing appropriate outbound controls, the systems acts as a good steward of federal and Internet network resources by reducing the risk to external electronic mail systems as well as providing a

monitoring interface for Data Loss Prevention (DLP) services, encompassing both spam and malware filtering of mail transfers. The outbound MTA functions are self-adjusting depending on the target external mail system and agency policy. For example, electronic mail between federal agencies may be handled differently than mail destined for Internet mail systems. Based on the findings of each function, the MTA will make a disposition decision for each outbound mail transaction. Depending on the agency security policy, the outbound MTA will opportunistically enable server-to-server encryption services wherever possible.

## **2.4 Bilateral Mail Relay/Exchanger (MTA)**

The bilateral mail exchanger provides an optional proxy capability which enables the pre-collection of electronic mail. Large sites may choose to employ a mail exchanger outside of their enclave which, in turn, routes mail to multiple inbound and outbound electronic mail gateways. This configuration provides a mechanism to outsource the mail exchange function as well as some mail pipeline functions. By implementing external mail exchangers, disaster recovery and business continuity functions are also supported by storing incoming and outgoing mail in a trusted location during enclave mail system outages.

## **2.5 Mobile Messaging**

Many agencies require connection to a mobile device mail system. For example, an agency may require Blackberry electronic mail services provided by a Blackberry Enterprise Server (BES) or Android/iOS services provided by the Microsoft ActiveSync protocol. (The reference architecture does not advocate any particular mobile messaging service but recognizes the prominent position of these protocols in the federal workplace.) Mobile messaging servers communicate via an external network to mobile devices and, in turn, the mobile messaging server sends and receives electronic mail via the inbound and outbound MTAs. The mail gateway reference architecture does not describe the mobile messaging architecture in detail except for the interface of the mobile architecture with the mail gateway pipeline.

# **3 Security Patterns**

The operation of the electronic mail gateway is described by first identifying common use cases then identifying the functions of the security architecture required to meet federal security requirements.

## **3.1 Security Use Cases**

### **3.1.1 Pattern 1: Inbound Electronic Mail**

The Inbound Electronic Mail security pattern consists of all inbound mail originating outside the agencies' enclave. The security pattern does not differentiate between electronic mail arriving from trusted or unknown sources. All mail will pass through an inbound pipeline and be processed by agency policy. The theory is that the inbound pipeline components are the same regardless of source.

### **3.1.2 Pattern 2: Outbound Electronic Mail**

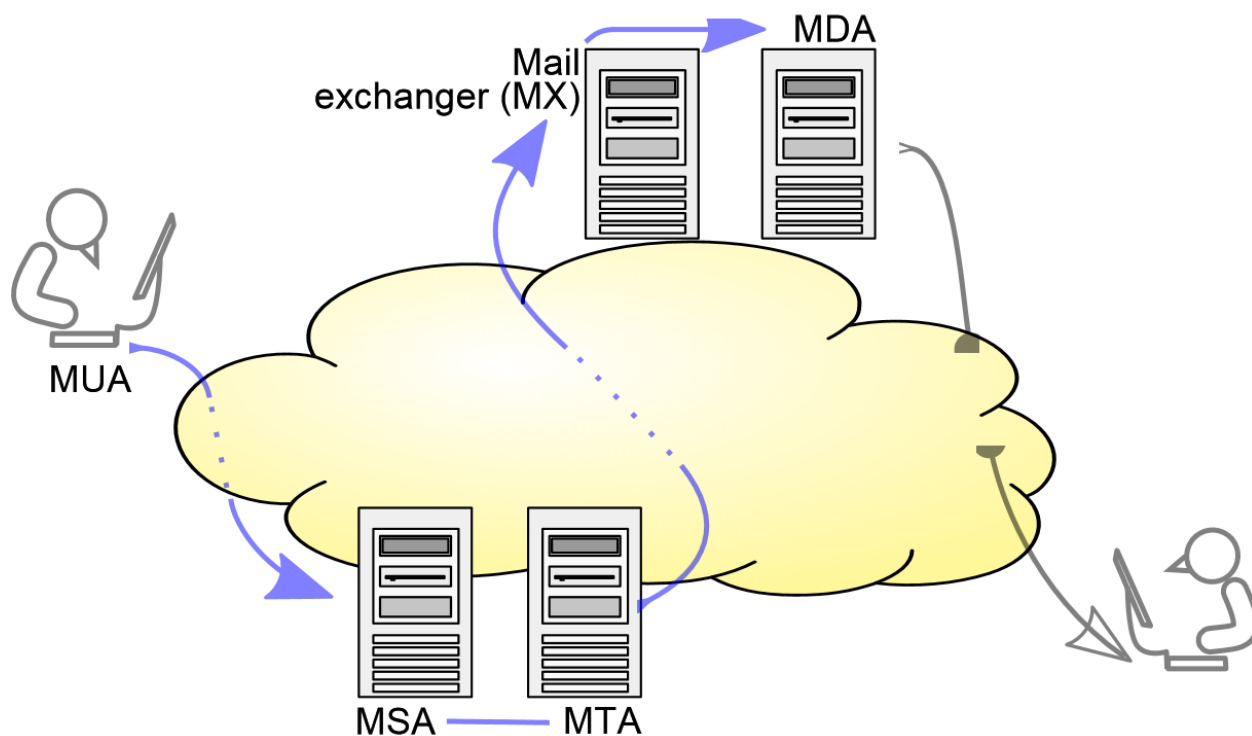
The Outbound Electronic Mail security pattern consists of all outbound electronic mail originating from within the sending agencies' enclave. This includes mail being sent to trusted, untrusted, or unknown trust level destinations. The operational concept is all outbound mail will pass through the same outbound pipeline. The pipeline might be tuned for specific destinations but the pipeline components will not change.

### **3.1.3 Pattern 3: Mobile Messaging**

The Mobile Messaging security pattern describes the condition where the electronic mail gateway needs to send or receive mail from a commercial mobile messaging system. The mobile messages must fully participate in the electronic mail gateway. The mobile messaging reference architecture will be described in a separate reference architecture but it is included here to describe the interaction with the electronic mail gateway reference architecture.

## **3.2 Security Architecture Components**

The normal flow of Simple Mail Transport Protocol (SMTP) mail is illustrated in Figure 2 below. Electronic mail gateways consist of both mail transfer agent (MTA) and Mail Exchanger (MX) functions implemented over one or more agency mail servers. Ideally mail server functions are divided over multiple redundant hosts to better assure high availability and security encapsulation.



**Figure 2 - SMTP Transfer model**

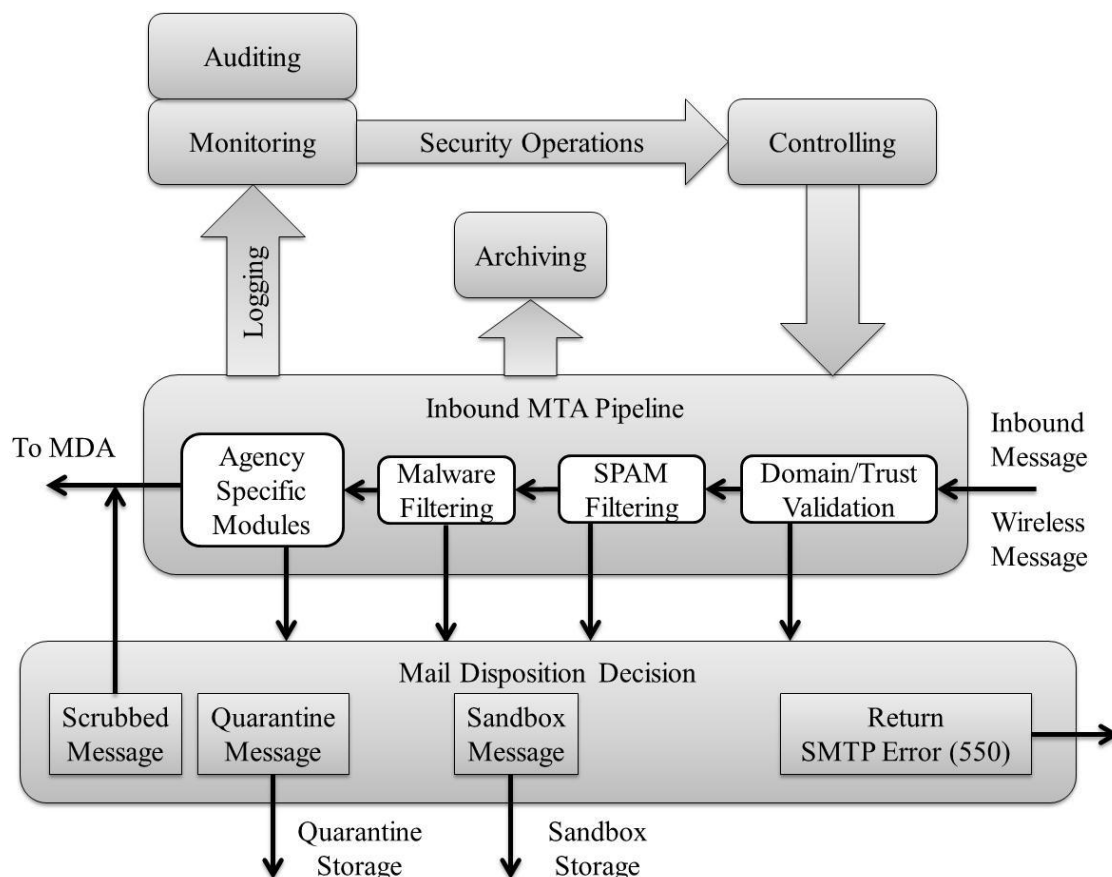
Because the functions of mail gateways are heterogeneous at the source and destination sites, they should be configured differently depending on whether they are to handle inbound or outbound electronic mail. It should also be noted that multiple hosts may be configured to perform each function depending on capacity requirements.

### 3.2.1 Pipeline Structure

The email gateway should be configured in a modular fashion which allows for the provision of additional mail security controls as well as redundant hosting of mail services. Incoming and outgoing mail must be routed through a pipeline architecture consisting of one or more servers performing the designated electronic mail handling functions.

A series of functions are performed on the message as it passes through an inbound or outbound MTA. The MTA provides anti-spam functions, data loss prevention, content compliance, malware detection, and domain validation. Depending on agency security policies, one or more additional functions can be inserted into the mail processing pipeline. Policy enforcement will also dictate what actions or logging is required for each pipeline component. A representation of an inbound and outbound MTA pipeline is shown in Figure 3 and 4. The advantage of a pipeline is that additional processes can be added and it is not constrained to a single vendor solution.

Depending on agency policies, the MTA pipelines should be linked to the agencies archiving functions and policies.



**Figure 3 - Inbound MTA Pipeline**

Also, in order to provide electronic mail gateway monitoring and control visibility, the MTA pipeline components must provide status information via logging to a monitoring function. The specific agency policies will dictate how the logging information is used but it is especially important to consider logging, monitoring, controlling, archiving, and auditing when outsourcing any function of the MTA pipelines.

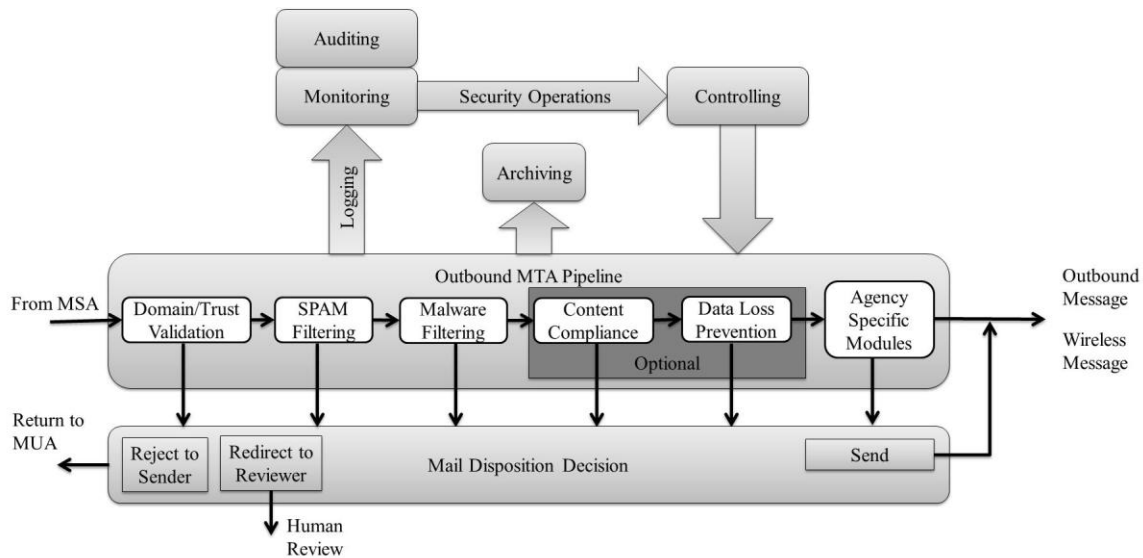
The order of pipeline functions is critical to the efficient operation of the pipeline. The design objective is to perform the most effective and least resource intensive functions first. In the case of the inbound pipeline, domain validation provides a quick method to filter incoming messages by the level of trust established by an individual sender. This necessitates making disposition decisions on each mail message as soon as possible.

The current proportion of SPAM received by a conventional inbound mail pipeline makes rejecting suspected SPAM early in the pipeline critical. By filtering SPAM early, fewer messages need to be processed by more resource-intensive malware filters. Many security vendors have developed sophisticated SPAM filters which are based on proprietary data collection techniques and it is important to note, the frequency of SPAM filter updates when choosing a vendor solution.

Because SPAM attackers have the option to run short-duration attacks which “fly under the radar” of update cycles, agency solutions need to use any bad IP address, domains, or filters published by the US CERT to make a mail disposition decision. The decision criteria will be based on agency policies as well as technical capabilities. At a minimum, the inbound pipeline will support scrubbing messages, quarantine, and the issuance of SMTP 550-series error messages. The SMTP 550 reply code is generic: “Requested action not taken: mailbox unavailable”. This reply condition provides minimal information to SPAM and malware senders but provides enough information to legitimate sending servers that something is wrong.

Each module in the inbound mail pipeline will either pass the message to the next module or execute a mail disposition event. Final disposition either results in the mail being rejected with a SMTP error code of 550, being moved to a quarantine, being scrubbed and delivered to the user, or being moved to a sandbox. The reject option must return a code of 550 to prevent the sender from being able to derive account information from the MTA. The quarantine and sandbox both prevent delivery of the message to the MUA but the handling of the message is different. In the case of quarantine, the message is stored and an appropriate message is delivered alerting the user on how to view the message without retrieving it. The sandbox opens the message trying to determine risk of any message content. If the message is determined to be safe the message can be returned to the user. The scrubbing option removes any detected problems and delivers the message to the MUA. As an example, the scrubber might remove an attachment that is deemed to be high risk and replace it with an appropriate message. A frequently seen case is the removal of executable attachments.

For the inbound pipeline all of the modules must be included. If a portion of the pipeline is outsourced, all modules must be accounted for using either outsourced or organic resources. The mail disposition instruction system must support the return function but the agency can implement any combination of the scrubbing, quarantining, or sandboxing of messages but at least one must be used.



**Figure 4 - Outbound MTA Pipeline**

The outbound pipeline also needs to be constructed with most effective and least resource intensive modules first. To control outbound electronic mail based on destination level of trust, the domain validation is performed early. In order to protect the destination electronic mail systems, SPAM and malware filtering are also performed early in the outbound pipeline.

The objective is to prevent the local enclave from forwarding any SPAM or malware issues. As an example, hosts in the agency enclave might be hijacked and included in a botnet like denial of service attack. By eliminating problematic electronic mail early, the more resource intensive content compliance and data loss prevention function will only process the minimum required messages.

The same rules identified in the outbound pipeline when identifying vendors for SPAM filtering modules. Based on the results of the pipeline functions, the outbound pipeline makes a mail disposition decision. The decision must be tunable based on agency policy. The available options are: reject to sender, redirect to a reviewer, or send. Since the sender is from inside the enclave, specific rejection conditions can be returned. The option of rejecting to a reviewer provides a mechanism to allow for human decisions. For example, the data loss prevention function might invoke the need for a human review. The send option permits the MTS to forward the message to the intended recipient. An important function of the outbound pipeline is to preserve the reputation of the agency when sending outbound messages.

The pipeline shows optional modules that can be plugged-in based on agency specific module. In Figure 4, the pluggable modules are annotated as optional and can be inserted as necessary. Any additional pluggable modules will be included as part of the agency specific module. For the outbound pipeline, all modules not marked as optional must be included. As with the inbound pipeline, outsourcing is possible but all modules must be accounted for in either the

outsourcing arrangements or by organic resources. For the mail disposition decision, the send and reject to sender options must be supported. The redirect to reviewer is optional based on specific agency policies.

### **3.2.2 Data Loss Prevention**

Data Loss Prevention (DLP) is the most important functional module in the outbound MTA pipeline. It sequesters the transfer of sensitive information via an electronic mail message from the internal enclave to a lower-trust network. DLP products and solutions are still evolving in commercial off-the-shelf solutions and are designed to identify, monitor, and prevent the movement of sensitive information via electronic mail which can also help reduce insider threat or data exfiltration by malware and viruses.

DLP solutions must be able to scan electronic mail attachments as well as text regardless of whether it is encrypted. During the scanning, high risk data is identified and protected by means of sequestration. The challenge lies in reducing false positives while minimizing data leakage. As a result, federal agencies implementing DLP modules must be able to describe both the types and format of data requiring sequestration using both Bayesian logic and Unix-style regular expressions. The agency also needs to determine what actions must be taken once a violation is detected. As a result, the DLP process needs to be tightly linked to agency risk remediation policies and the selection of a specific DLP will also have implications as to how an MTA is configured.

### **3.2.3 Content Compliance**

The content compliance module will look for electronic mail content in the outbound pipeline which does not comply with agency policies. In the context of the mail gateway architecture, content compliance is a decision based exclusively upon the types of content being distributed and not the actual content itself. For example, an agency policy might preclude sending attached images, video or executable files. The content compliance module looks at the file type not the content of the specific image and sequesters illegal content whereas the DLP module inspects otherwise legal content.

### **3.2.4 Malware Filtering**

The malware filtering function is performed in both inbound and outbound MTA pipelines.

If the inbound MTA detects malware or viruses, the infected item must be moved into quarantine or deleted. In both cases, the event must be logged. The quarantined item could be the full message plus attachments or just the infected element. The location of the quarantine is not a function of the mail gateway architecture per se, but is a standalone application whose data is

supplied by the mail gateway architectures. Most implementations are done via web application or mail delivery agent modules.

For the outbound MTA, the malware filter module will send content to the reject processing decision handler. Agency rules will then determine if any components of the infected message are returned to the MUA or forwarded to the final destination with appropriate controls. In either case, the event must be logged and available to security administrators.

### **3.2.5 Domain Validation**

Domain validation is performed by both the inbound and outbound MTA pipelines. This module determines the level of trust inherent to a given message sender's domain. This is accomplished using a combination of techniques ranging from black and white lists to SPF/DKIM records as well as the IP addresses of the mail originator.

Based on this status, an electronic mail message will be sent or modified according to agency policy. For example, if an untrusted sender domain is detected, the mail message may be returned to sender, dropped, or quarantined.

Domain Name System Security Extensions (DNSSEC), DomainKeys Identified Mail (DKIM), or Sender Policy Framework (SPF) extensions to the DNS can be used to validate domains and correlate them with IP addresses. If none of these technologies are implemented, a domain validating MTA may "fall back" to a simple white list or black list. In either case, domain validation will be critical to making other policy decisions regarding the delivery of mail.

### **3.2.6 SPAM Filtering**

SPAM filters look for patterns in electronic mail and compare them with known and likely Spam signatures. The filtering techniques include a variety of approaches used in combination and are updated frequently. Electronic mail which is flagged as spam must be marked and either quarantined or deleted. Spam filtering is a critical component of the inbound MTA pipeline to reduce both denial of service (DoS) and phishing attacks and must evolve rapidly as commercial detection capabilities improve. This is a function which is commonly outsourced.

### **3.2.7 Agency Specific Modules**

The provision of modular services along the inbound and outbound MTA architecture allows agencies to implement a variety of additional modules depending on agency policy or specific filtering requirements.

### **3.3 Security Requirements**

#### **3.3.1 Inbound Gateway Mail Transfer Agent (MTA) Requirements**

In addition to high availability, an inbound MTA:

- Must include hot failover.
- Must be addressable by external networks (such as the public internet) and must be located in a network “demilitarized zone” (DMZ).
- Must support SMTPS transfers from outside domains opportunistically as well as unencrypted transfers from lower trust domains.
- Must be able to decode both Secure/Multipurpose Internet Mail Extensions (S/MIME) and/or Open Pretty Good Protection (OpenPGP) attachments.
- Must be able to query external DNS to obtain the SPF and/or DKIM key records associated with each incoming message.
- Must be able to verify DKIM signatures found on inbound electronic mail by querying external DNS information and verifying the cryptographic hash.
- Must be both fast and robust relative to the mail volume.
- Must be configured to deliver messages to one or more authorized internal mail delivery/transfer agents (MDAs/MTAs) as well as mail quarantine stores.
- Must be able to send SMTP mail to internal networks on port 25 in order to modularize mail-filtering transfer agents before finally delivering mail to user account mailboxes.
- Must be able to enforce agency specific security policies and be able to apply unique policies for individual source domains, permitting the mail transfer agent to enforce different security policies between federal organization, internet mail systems, or different enclaves.

#### **3.3.2 Outbound Gateway Mail Transfer Agent (MTA) Requirements**

In addition to appropriate capacity planning issues, an outbound MTA :

- Must be configurable to accept messages from one or more authorized internal mail submission agents (MSAs).
- Must be able to address external networks (such as the public internet) and therefore should also be located in an agencies DMZ.
- Must be configured to act exclusively as a relay for trusted MSAs and deny relay service to external mail systems.
- Must support the inclusion of RFC4871 compliant DKIM signature headers.

- Must be configurable to insert an RFC5322-compliant message header field to all outbound messages in its store and forward queue which encapsulates the RFC 1034 compliant domain name information of the sending/authorizing domain.
- Must be able to encode SDID public keys or obtain them from a local key server.
- Must support secure transactions with other network services including network time synchronization servers, data loss prevention tools and security log analysis tools such as network security event information managers (SEIMs).
- Must support transport layer security encryption via SMTPS for communication with capable recipients and be able to enforce agency specific security policies and be able to apply unique policies for individual destination domains.

### **3.3.3 Mail Submission Agent Requirements**

MSAs must reside behind network firewalls and be configurable to forward all non-local mail to an outbound Mail Transfer Agent located either in the network DMZ or the inside perimeter firewall.

### **3.3.4 Mail Delivery Agent Requirements**

Mail Delivery Agents receive mail from Mail Transfer Agents and therefore must be configurable to accept mail only from an inbound mail transfer agent and able to securely interact with local mail user agents (MUAs) over known ports via known protocols.

### **3.3.5 Mail User Agent Requirements**

Mail User Agents (MUAs) must be able to:

- Create and pass on RFC compliant mail headers and must be configurable to support SMTP over port 587 for mail submission as specified in RFC 4409.
- Interact securely with agency directory servers and mail quarantine servers.

### **3.3.6 Domain Name System (DNS) Requirements**

Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS. Therefore DNSSEC may be regarded as a pre-requisite for trusted mail identification on the internet, however the implementation of DKIM and SPF render email attacks more difficult even in the absence of DNSSEC secured DNS records.

In addition, external facing authoritative name servers must be able to:

- Respond to queries for DKIM public keys.
- Support the resolution of type 99 SPF records for all authorized outbound mail transfer agents within the agency administrative domain.
- Deliver RFC 4408-compliant Sender Policy Framework authorized mail server designations for all authorized mail transfer/exchange agents.
- Internal-facing authoritative name servers must be able to respond to queries for DKIM public keys.
- Internal recursive name servers must be able to issue recursive requests for DKIM and SPF compliant DNS records.

### **3.3.7 Firewall Requirements**

Agency perimeter firewalls must be able to:

- Forward incoming SMTP mail on port 25 only to inbound MTAs.
- Block all other incoming ports from external networks directed to internal MTAs.
- Block all internal port 25 requests that do not originate from an MTA directed to an external server.
- Allow port 53 DNS recursion for outbound MTAs.
- Allow port 587 for internal mail submission.
- Based on agency policy, allow port 587 connections from MUAs originating from outside the enclave (it is strongly recommended this be prevented and a secure VPN connection be used instead).
- Allow port 80 or port 443 to the agency OCSP responder (the port is determined by the configuration of the OCSP server).
- Allow port 102 for the X.400 connector if external X.400 connections are required.

### **3.3.8 Logging Requirements**

The mail gateway components must be able to:

- Gather and report statistical information for messages transferred inbound and outbound.
- Message logs must contain system health information, security policy violations, source and destination domain statistics, malware/virus detection and quarantine, server load levels, failures in mail gateway functionality, and DNS event errors.
- Comply with SEIM input queue requirements in accord with TIC Reference Architecture v2 logging functional requirement.

### 3.3.9 System Monitoring and Control

All mail gateway components must be able to:

- Log and send information to a security event information management system (SEIM).
- Minimum expected logging functions include Simple Network Management Protocol (SNMP) and/or Unix syslog functions but must also be configurable and extensible to meet specific risk profiles and electronic mail gateway control requirements and policies. The requirements for system monitoring and control need to be included in any outsourcing arrangement.

#### 3.3.10 Archiving Requirements

- Inbound and outbound MTAs must provide archiving capability to align with agencies' electronic mail archiving policies (though archiving function can be satisfied by components outside the MTA pipeline).
- Individual agency policies determine if the MTA, MDA, MSA, and MUA should also archive the mail messages but the consolidation of those determinations into a formal archiving policy is imperative.
- MTAs do not perform an archiving storage function, but rather link to external archival systems.
- The MTA will host only internal log system logs. All other logs will be recorded and stored elsewhere (such as a network SEIM).

#### 3.3.11 Audit Requirements

- In support of the federal and agency auditing requirements, the electronic mail gateway components must collect and provide access to auditing information.
- The transmission of transaction logs to external auditing systems must be either via electronic mechanism or human analysis of auditing, logging, and configuration data. This enables access to the information required to comply with FISMA and OMB security mandates.

## 4 Systemic Threats & Mitigations

A catalog of key threat types is listed in this section along with strategies for mitigating the threat type. See also RFC 4686.

Threat	Description	Impact	Mitigation
--------	-------------	--------	------------

Denial of Service (DoS) attack against inbound MTA	DoS can be initiated intentionally either malicious attacker or unintentionally by a valid user/system.	Agency email can be disrupted or denied.	Hardened port firewalls should be combined with dedicated layer 7 firewalls to minimize DoS impact.
Denial of Service (DoS) attack against Key service	DoS can be initiated against DNS servers providing DKIM & SPF record information.	Agency email can be disrupted or denied.	DNS queries should be restricted to external nameservers; hardened port firewalls should be combined with dedicated layer 7 firewalls to protect DNS servers; inbound MTAs should use dedicated key serving resources.
Malware/virus infected mail message	Internal hosts can be compromised or rendered inoperable by malware passing through the email pipeline.	Any or all agency computing functions can be disrupted or denied.	Strict inbound mail filtering should be implemented using hardened appliances and/or third party services. Enclosures should be unpacked prior to delivery.
Malevolent hyperlink /“Phishing”	Internal hosts can be compromised or rendered inoperable by deceptive passing through the email pipeline which leads to the installation of malware or viruses.	Any or all agency computing functions can be disrupted or denied.	Strict inbound mail filtering should be implemented using hardened appliances and/or third party services. DNS blacklisting should be combined with link sequestration and proxy services to minimize threat.
Man-in-the-middle attack/	External upstream hosts are configured to queue mail for external domains from outside hosts.	Agency email can be disrupted, disclosed or denied.	Implement DNSSEC extensions and SPF framework to control MX record deployment ( <i>See Appendix A</i> ).

DNS Spoofing	Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS.	Agency email can be disrupted, disclosed or denied.	Implement DNSSEC extensions.
Unwanted electronic mail ("Spam")	Agency computing resources are wasted handling unwanted and unsolicited email.	User time is wasted and agency storage is wasted.	Establish rule-based mail filtering with real-time blacklist sensitivity; check for SPF and DKIM records from mail source.
Damaged or corrupted electronic mail	Mail is incorrectly transmitted to its destination due to failures in the MTA pipeline.	Agency email can be disrupted, disclosed or denied.	Closely monitor and log all MTA activity; apply vendor recommended patches and use message integrity checking where available.
Reputation Attacks	Forged outbound email may be used to damage the credibility or reputation of the agency.	Agency credibility is damaged.	Implement DNSSEC, DKIM and SPF extensions ( <i>See Appendices A&amp;B</i> )
Reflection Attacks	Intentionally mis-addressed messages are sent to third party MTAs, causing it to be "bounced" or sent to the return address on the message. The forged sender address then becomes the target of the "returned message".	Agency email can be disrupted or denied.	Establish rule-based mail filtering with real-time blacklist sensitivity; check for SPF and DKIM records from mail source and implement DKIM/SPF DNS extensions to prohibit return mail from outside sources ( <i>See Appendices A&amp;B</i> )

Theft of internal mail addresses	Recipient MTAs are tested for common names in order to identify targets for phishing attacks.	Sensitive agency information may be disclosed.	Do not return mail messages and provide only 500-series message fail notice; implement Bayesian anti-spam controls with real-time blacklist addition capability to discourage probing.
Verification Probe Attack	An extension of a mail probe is to send a message with a DKIM signature to many addresses without valid signatures and with a different selector. The attacker then monitors key service requests to determine which selectors had been accessed and which addressees used DKIM verification.	Sensitive agency information may be disclosed.	Place key servers behind firewalls and allow communication only with authorized hosts.
Relationship Exploitation	Forged email from familiar sender addresses is more likely to be acted upon by a recipient. Malware or spam may be delivered via this method.	Agency email can be disrupted, disclosed or denied.	Implement strict inbound mail filtering using hardened appliances and/or third party services. Enclosures should be unpacked prior to delivery and mail sources should be checked against SPF and DKIM records as well as real-time blacklists.

Signed message replay	Signed messages are retransmitted by an attacker to additional recipients beyond those intended by the original author. The attacker first receives a legitimate message from the victim and then retransmits it intact but with different envelope addresses in order to deliver unwanted email or malware.	Any or all agency computing functions can be disrupted or denied.	Implement both DKIM and SPF records along with DNSSEC extensions to prevent re-use of credentials from unauthorized sources ( <i>See Appendices A&amp;B</i> ).
Chosen message replay	An attacker may create a message and obtain a valid signature by sending it through an MTA authorized by the originating domain. They then "replay" the signed message by sending it, using different envelope addresses, to a large number of other recipients.	Sensitive agency information may be disclosed.	Implement both DKIM and SPF records along with DNSSEC extensions to prevent re-use of credentials from unauthorized sources.
Packet Amplification Attacks	By requiring substantially larger DNS payload replies, DKIM contributes to denial-of-service attacks involving the transmission of spoofed UDP DNS requests to openly-accessible domain name in which the response from the name server is larger than the request, thereby forcing the name server to function as an amplifier for such an attack.	Agency email can be disrupted or denied.	Place public-facing DNS servers behind port firewalls using real-time blacklisting and stateful packet inspection; throttle responses based on service throughput.

False positives	Mail gateway incorrectly identifies legitimate mail as spam or malware.	Agency email can be disrupted, ignored or denied.	Implement spam quarantine inspection to facilitate manual spam validation.
Encryption weaknesses	Either weak or improperly configured encryption strategies are used.	Agency email can be compromised, corrupted, or source incorrectly identified.	Use FIPS certified encryption protocols whenever possible.

## 5 Security Configuration

Recommendation	Description	Key Benefits
Electronic mail gateways should be part of a unified mail-handling GSS under FISMA.	As an essential support system email should be consider holistically from a FISMA security standpoint.	More effective administration and monitoring of essential agency IT functions.
DNSSEC should be implemented prior to DKIM/SPF	Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS.	More robust and secure agency information services.
SPF rules should be implemented irrespective of DKIM as part of transition	Because SPF provides useful anti-spam capabilities that do not require strict identity establishment, it can be considered a useful transitional step forward to improving network identity services.	Better anti-spam/phishing controls.

## 6 Appendix A: Sample SPF Records

SPF domains have to publish at least two directives: a version identifier and a default mechanism. The simplest possible SPF record looks like the following:

```
agency.gov. TXT "v=spf1 -all"
```

This declaration means that *agency.gov* never sends mail. A domain which is only used for web services might have an SPF declaration such as this, but most domains will want to designate permitted hosts using one or more mechanisms.

If your MX servers send mail, you should designate them like this:

```
agency.gov. TXT "v=spf1 mx -all"
```

In this example, if *agency.gov* had an MX record, its MX servers would be designated as valid mail sources. If other machines in the domain also send mail, designate them as follows:

```
agency.gov. TXT "v=spf1 mx ptr -all"
```

This designates all the hosts whose PTR hostname match *agency.gov*. If any other machines not in the domain also send mail from that domain—such as, for example, a hosted mail solutions provider, designate them like this:

```
agency.gov. TXT "v=spf1 a:agency.gov mx ptr -all"
```

Each of your mail servers should have an SPF record also and consider creating an SPF record for every other machine in your domain.

Spammers can forge hostnames as well as domain names: to SMTP there is no difference between the two. If they start forging the hostnames of web servers, unix servers, even workstations, you'll want to create SPF records for those machines also.

If you send mail through another organization's servers, you should use an Include directive to point to their servers.

If other domains use exactly the same set of hosts, you can set up redirects for them. "Redirect" aliases point to other domains which themselves publish SPF records. This aliasing mechanism makes it possible to easily consolidate multiple domains that share the same set of designated hosts.

For more information see: <http://www.openspf.org/>

## 7 Appendix B: Sample DKIM domain record entry

DKIM is anti-spam/phishing method which works by signing outbound e-mail messages with a cryptographic signature which can be verified by the recipient to determine if the messages originate from an authorized system.

The process of signing outbound messages and verifying this signature is typically done by the e-mail servers at each end - not by end-users client software. DKIM uses DNS TXT-records to define policy and public encryption keys for a domain name.

The public key value is typically generated by a function in the e-mail server software or by using a tool such as "openssl". The public key must of course match the private key used by the e-mail server software to sign outgoing messages.

There are basically two types of DNS records used by DKIM; policy records and public key records.

Policy records:

A domain name using DKIM should have a single policy record configured.

This is a DNS TXT-record with the name "`_domainkey`" prefixed to the domain name - for example:

```
"_domainkey.agency.gov".
```

The simplest DKIM DNS entry looks like this:

```
sitename._domainkey.agency.gov IN TXT  
"v=DKIM1; p=mypublickeygoeshere; s=email"
```

In this example, *sitename* is the name of the authorized mail transfer agent for *agency.gov* and the public portion of the domain key follows the `p=` designator.

The data of this TXT-record contains the policy which is basically either "`o=-`" or "`o=~`". "`o=-`" means "all e-mails from this domain are signed", and "`o=~`" means "some e-mails from this domain are signed". Additional fields for test (t), responsible e-mail address (r), and notes (n) may also be included - for example "`o=-; n=some notes`".

Receiving e-mail servers check this policy record to find out to what extent the sender domain name uses DKIM, if there is no such record, the domain does not support DKIM and it cannot be used to validate mail. Based on the stipulated policy, the receiving e-mail server might reject or flag un-signed messages from this domain name.

## 2) Public key records:

An e-mail message signed with DKIM will include a header item "DomainKey-Signature" containing the cryptographic signature and a few other fields including a "selector" (s=) - for example:

```
DomainKey-Signature: a=rsa-sha1;  
s=sitename;  
d=agency.gov;  
c=simple;  
q=dns;  
b=dydVyOfAKCdLXdJOc8G2q8LoXS1EniSbav+yuU4zGffruD00lszZVoG4ZHRNiY  
zR;
```

For the receiving e-mail server to verify this signature, it must first obtain the public key for the selector value. For above example, this is stored in a DNS TXT-record with the name "sitename.\_domainkey.agency.gov".

In other words, the name of this TXT-record is the selector (s=...) + .\_domainkey. + the domain name.

The data of this TXT-record is in the format "k=rsa; p=MHww..." where value after p= is the public key. Additional fields for granularity (g), test (t), and notes (n) may also be included depending on individual requirements.

The selector value ("*sitename*" in above example) may be a fixed value used by your e-mail server software, or you may be able to configure multiple selectors for example for different branch offices or individual e-mail servers. The important thing is that for each selector used to sign outgoing messages from your domain name, you setup a separate TXT-record in DNS.

## **8 Appendix C: Acronyms – Common Abbreviations**

**BES** – Blackberry Enterprise Server

**CIO** - Chief Information Officer

**D/A** - Department/Agency

**DHS** - Department of Homeland Security

**DLP** – Data Loss Prevention

**DMZ** – Demilitarized Zone

**DKIM** - DomainKeys Identified Mail

**DNS** - Domain Name System

**DNSSEC** - Domain Name System Security Extensions

**DoS** - Denial of Service

**FIPS** - Federal Information Processing Standards

**FISMA** - Federal Information Security Management Act

**FNS** - Federal Network Security Branch

**IP** - Internet Protocol

**NIST** - National Institute of Standards and Technology

**NSTIC** – National Strategy for Trusted Identities in Cyberspace

**MTA** – Mail Transfer Agent

**MSA** – Mail Submission Agent

**MDA** – Mail Delivery Agent

**MUA** – Mail User Agent

**MX** – Mail Exchange

**OCSP** – Online Certificate Status Protocol

**OMB** - Office of Management and Budget

**PKI** - Public Key Infrastructure

**RFC** – Request For Comment

**SDID** – Secure Digital Identification

**S/MIME** - Secure/Multipurpose Internet Mail Extensions

**SEIMs** - Security Event Information Managers

**SPF** - Sender Policy Framework

**SMTP** - Simple Mail Transfer Protocol

**SMTPS** – Simple Mail Transfer Protocol Secure

**SNMP** - Simple Network Management Protocol

**TCP** - Transmission Control Protocol

**TIC** - Trusted Internet Connections

**UDP** - User Datagram Protocol

**UTA** – User Transfer Agent

**VPN** – Virtual Private Network

## 9 Appendix D: Glossary – Common Terms and Definitions

**Address Resolution Protocol (ARP)** – A protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the Internet Protocol (IP) address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted to it.

**Body** – The section of an email message that contains the actual content of the message.

**Demilitarized Zone (DMZ):** The DMZ (or Service Network) is a perimeter network segment that enforces the internal network information assurance policy for external information exchange.

**Denial of Service (DoS):** Intentionally or unintentionally overloading a computer resource to make a service unavailable.

**Domain Name System (DNS):** DNS is a hierarchical, distributed database for any resource connected to the Internet or private network that translates readable domain names to IP addresses.

**Domain Name System Security Extensions (DNSSEC):** DNSSEC is a suite of specifications that provides origin authentication, authenticated denial of existence, and data integrity to DNS clients (resolvers). DNSSEC was designed to prevent cache poisoning and does not provide services for availability or confidentiality.

**Header** – The section of an email message that contains vital information about the message, including origination date, sender, recipient(s), delivery path, subject, and format information. The header is generally left in clear text even when the body of the email message is encrypted.

**Internet Message Access Protocol (IMAP)** – A mailbox access protocol defined by IETF RFC 3501. IMAP is one of the most commonly used mailbox access protocols. IMAP offers a much wider command set than POP.

**Intrusion Detection and Prevention System (IDS/IPS or IDPS):** Identifies potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

**Local Delivery Agent (LDA)** – A program running on a mail server that delivers messages between a sender and recipient if their mailboxes are both on the same mail server. An LDA may also process the message based on a predefined message filter before delivery. See also Mail Delivery Agent and Mail User Agent.

**Mail Server** – A host that stores incoming mail for distribution to users and forwards outgoing mail. The term may refer to just the application that performs this service, which can reside on a machine with other services, but for this document the term refers to the entire host including the mail server application, the host operating system and the supporting hardware.

**Mail Server Administrator** – The mail server equivalent of a system administrator. Mail server administrators are system architects responsible for the overall design and implementation of mail servers.

**Mail Delivery Agent** -- Mail Delivery Agents receive mail from Mail Transfer Agents

**Mail Submission Agent** – Mail Submission Agents forward all non-local mail to an outbound Mail Transfer Agent

**Mail Transfer Agent (MTA)** – A program running on a mail server that receives messages from mail user agents or other MTAs and either forwards them to another MTA or, if the recipient is on the MTA, delivers the message to the local delivery agent (LDA) for delivery to the recipient. Common MTAs include Microsoft Exchange and sendmail.

**Mail User Agent (MUA)** – A mail client application used by an end user to access a mail server to read, compose, and send email messages. Common MUAs include Microsoft Outlook and Mozilla Thunderbird.

**Malware** – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

**Multipurpose Internet Mail Extensions (MIME)** – A protocol that makes use of the headers in an IETF RFC 2822 message to describe the structure of rich message content.

**Network Administrator** – A person who manages a network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

**Open Pretty Good Privacy (OpenPGP)** – A protocol defined in IETF RFCs 2440 and 3156 for encrypting messages and creating certificates using public key cryptography. Most mail clients do not support OpenPGP by default; instead, third-party plug-ins can be used in conjunction with the mail clients. OpenPGP uses a “web of trust” model for key management, which relies on users for management and control, making it unsuitable for medium to large implementations.

**Operating System** – The software “master control application” that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The operating system sets the standards for all application

programs (such as the mail server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.

**Patch** – An immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

**Phishing** – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

**Post Office Protocol (POP)** – A mailbox access protocol defined by IETF RFC 1939. POP is one of the most commonly used mailbox access protocols.

**Secure Multipurpose Internet Mail Extensions (S/MIME)** – A protocol defined in IETF RFCs 3850 through 3852 and 2634 for encrypting messages and creating certificates using public key cryptography. S/MIME is supported by default installations of many popular mail clients. S/MIME uses a classic, hierarchical design based on certificate authorities for its key management, making it suitable for medium to large implementations.

**Simple Mail Transfer Protocol (SMTP)** – An MTA protocol defined by IETF RFC 2821. SMTP is the most commonly used MTA protocol.

**Spam** – Unsolicited bulk commercial email messages.

**Spyware** – Malware intended to violate a user's privacy.

**System Administrator** – A person who manages a computer system, including its operating system and applications. Responsibilities are similar to that of a network administrator.

**Transmission Control Protocol (TCP):** TCP provides reliable, ordered delivery of a stream of bytes on an Internet Protocol (IP) network from a program on one computer to another program on another computer. TCP, along with UDP, are the two core Network Protocols in the Internet Protocol Suite.

**User Datagram Protocol (UDP):** UDP allows computer applications to send messages (datagrams) to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. UDP, along with TCP, are the two core Network Protocols in the Internet Protocol Suite.

**Vulnerability** – A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version numbers of software. Each vulnerability can potentially compromise the system or network if exploited.

## **10 Appendix E: Selected Existing Guidance**

### **10.1 LEGISLATION**

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

### **10.2 POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA**

National Security Presidential Directive (NSPD) 54, *Cyber Security and Monitoring*, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, *Computer Network Monitoring and Cyber-security*, 8 January, 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, 2 August 2005.

Office of Management and Budget (OMB) Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, 11 January 2007.

Office of Management and Budget (OMB) Memorandum M-08-05, *The Trusted Internet Connection initiative (TIC)*, November 2007.

National Security Telecommunications And Information Systems Security Committee NTTISSP 101, *National Policy on Securing Voice Communications*, 14 September 1999.

### **10.3 STANDARDS**

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

General Services Administration (GSA), Public Buildings Service (PBS), *Facilities Standards (P100)*, 2009.

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Module*, 3 December 2002.

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

IEEE 802.1X: IEEE Standard for port-based Network Access Control (PNAC).

## 10.4 GUIDELINES

NIST's Information Technology Laboratory, ITL Security Bulletins, *An Introduction to Secure Telephone Terminals - ITL Security Bulletin*, March 1992.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, December 2010.

National Institute of Standards and Technology Special Publication 800-81, Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, April 2010.

National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

Office of Management and Budget Memoranda, M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, 4 April 2008.

Office of Management and Budget Memoranda, M-08-26, *Transition from FTS 2001 to NETWORX*, 28 August, 2008.

Office of Management and Budget Memoranda, M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, 20 September 2008.

Office of Management and Budget Memoranda, M-09-32 *Update on the Trusted Internet Connections Initiative*, 17 September 2009.

[Messaging Anti-Abuse Working Group, \(MAAWG\) Best Common Practices for Mitigating Abuse of Web Messaging Systems, August 2010](#)

## 10.5 IETF RFCs

- [Kohnfelder] Kohnfelder, L., "Towards a Practical Public-key Cryptosystem", May 1978.
- [RFC0989] Linn, J. and IAB Privacy Task Force, "[Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures](#)", RFC 989, February 1987.
- [RFC1034] Mockapetris, P., "[Domain names - concepts and facilities](#)", STD 13, RFC 1034, November 1987.
- [RFC1113] Linn, J., "[Privacy enhancement for Internet electronic mail: Part I - message encipherment and authentication procedures](#)", RFC 1113, August 1989.
- [RFC1848] Crocker, S., Galvin, J., Murphy, S., and N. Freed, "[MIME Object Security Services](#)", RFC 1848, October 1995.
- [RFC1991] Atkins, D., Stallings, W., and P. Zimmermann, "[PGP Message Exchange Formats](#)", RFC 1991, August 1996.
- [RFC2440] Callas, J., Donnerhackle, L., Finney, H., and R. Thayer, "[OpenPGP Message Format](#)", RFC 2440, November 1998.
- [RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "[MIME Security with OpenPGP](#)", RFC 3156, August 2001.
- [RFC3851] Ramsdell, B., "[Secure/Multipurpose Internet Mail Extensions \(S/MIME\) Version 3.1 Message Specification](#)", RFC 3851, July 2004.
- [RFC4406] Lyon, J. and M. Wong, "[Sender ID: Authenticating Electronic mail](#)", RFC 4406, April 2006.
- [RFC4407] Lyon, J., "[Purported Responsible Address in Electronic mail Messages](#)", RFC 4407, April 2006.
- [RFC4408] Wong, M. and W. Schlitt, "[Sender Policy Framework \(SPF\) for Authorizing Use of Domains in Electronic mail, Version 1](#)", RFC 4408, April 2006.
- [RFC4686] Fenton, J., "[Analysis of Threats Motivating DomainKeys Identified Mail \(DKIM\)](#)", RFC 4686, September 2006.
- [RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "[DomainKeys Identified Mail \(DKIM\) Signatures](#)", RFC 4871, May 2007.
- [RFC4880] Callas, J., Donnerhackle, L., Finney, H., Shaw, D., and R. Thayer, "[OpenPGP Message Format](#)", RFC 4880, November 2007.
- [RFC5322] Resnick, P., Ed., "[Internet Message Format](#)", RFC 5322, October 2008.